

**No. 25-1411**

---

**IN THE UNITED STATES COURT OF APPEALS  
FOR THE FOURTH CIRCUIT**

---

AMERICAN FEDERATION OF STATE, COUNTY AND MUNICIPAL  
EMPLOYEES, AFL-CIO, et al.,

Plaintiffs-Appellees,

v.

SOCIAL SECURITY ADMINISTRATION, et al.,

Defendants-Appellants.

---

On Appeal from the United States District Court  
for the District of Maryland

---

**REPLY BRIEF FOR APPELLANTS**

---

BRETT A. SHUMATE,

*Assistant Attorney General*

YAAKOV M. ROTH

*Principal Deputy Assistant*

*Attorney General*

ERIC D. MCARTHUR

*Deputy Assistant Attorney General*

BRAD HINSHELWOOD

JACK STARCHER

SIMON JEROME

JACOB CHRISTENSEN

*Attorneys, Appellate Staff*

*Civil Division, Room 7515*

*U.S. Department of Justice*

*950 Pennsylvania Avenue NW*

*Washington, DC 20530*

*(202) 514-8877*

---

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION .....	1
ARGUMENT .....	2
I. Plaintiffs Have No Likelihood of Success on the Merits .....	3
A. Plaintiffs fail to establish cognizable Article III injury .....	3
B. Plaintiffs do not challenge any final agency action reviewable under the Administrative Procedure Act.....	12
C. Plaintiffs’ Privacy Act and APA claims fail on the merits .....	18
1. Privacy Act claim .....	18
2. Arbitrary and capricious claim .....	30
II. Plaintiffs Also Fail to Establish the Remaining Preliminary Injunction Factors .....	33
CONCLUSION .....	35
CERTIFICATE OF COMPLIANCE	
CERTIFICATE OF SERVICE	

## TABLE OF AUTHORITIES

<b>Cases:</b>	<b><u>Page(s)</u></b>
<i>AFT v. Bessent</i> , No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025) .....	9
<i>Bennett v. Spear</i> , 520 U.S. 154 (1997) .....	16
<i>Bigelow v. Department of Def.</i> , 217 F.3d 875 (D.C. Cir. 2000), <i>cert. denied</i> , 532 U.S. 971 (2001) .....	25, 26
<i>City of New York v. U.S. Dep’t of Def.</i> , 913 F.3d 423 (4th Cir. 2019) .....	13
<i>Garey v. James S. Farrin, P.C.</i> , 35 F.4th 917 (4th Cir. 2022) .....	6, 7, 8
<i>Hearst Radio, Inc. v. FCC</i> , 167 F.2d 225 (D.C. Cir. 1948) .....	12
<i>Independent Equip. Dealers Ass’n v. EPA</i> , 372 F.3d 420 (D.C. Cir. 2004) .....	12
<i>Krakauer v. Dish Network, LLC</i> , 925 F.3d 643 (4th Cir. 2019) .....	6, 7
<i>Nken v. Holder</i> , 556 U.S. 418 (2009) .....	2
<i>Ohio Valley Env’t Coal v. Aracoma Coal Co.</i> , 556 F.3d 177 (4th Cir. 2009) .....	30
<i>O’Leary v. Trusted ID, Inc.</i> , 60 F.4th 240 (4th Cir. 2023) .....	9
<i>Parks v. U.S. IRS</i> , 618 F.2d 677 (10th Cir. 1980) .....	21
<i>Powers v. Ohio</i> , 499 U.S. 400 (1991) .....	6

<i>Seila Law LLC v. CFPB</i> , 591 U.S. 197 (2020) .....	22
<i>Social Sec. Admin. v. American Fed’n of State, Cnty., &amp; Mun. Emps.</i> , 145 S. Ct. 1626 (2025) .....	1
<i>Spokeo, Inc. v. Robins</i> , 578 U.S. 330 (2016) .....	3
<i>TransUnion LLC v. Ramirez</i> , 594 U.S. 413 (2021) .....	3, 11
<i>Tureen v. Equifax, Inc.</i> , 571 F.2d 411 (8th Cir. 1978) .....	5, 8
<i>Venetian Casino Resort, LLC v. EEOC</i> , 530 F.3d 925 (D.C. Cir. 2008) .....	14, 16
<i>Winter v. Natural Res. Def. Council, Inc.</i> , 555 U.S. 7 (2008) .....	2
 <b>U.S. Constitution:</b>	
Art. II, § 1, cl. 1 .....	22
Art. II, § 3 .....	22
 <b>Statutes:</b>	
5 U.S.C. § 551(13) .....	12, 15
5 U.S.C. § 552a(b)(1) .....	21, 27
5 U.S.C. § 552a(g)(1)(D) .....	17
5 U.S.C. § 552a(g)(4) .....	17
5 U.S.C. § 552a(i)(1) .....	7, 17
5 U.S.C. § 2105(a)(1)(A) .....	29
5 U.S.C. § 2105(a)(1)(D) .....	29

5 U.S.C. § 2105(a)(2)	29
5 U.S.C. § 2105(a)(3)	29

**Regulatory Material:**

Exec. Order No. 14,158, 90 Fed. Reg. 8441 (Jan. 29, 2025):	
§ 3(b), 90 Fed. Reg. at 8441	30
§ 3(c), 90 Fed. Reg. at 8441	29
§ 4(a), 90 Fed. Reg. at 8441	20, 22
§ 4(a)-(b), 90 Fed. Reg. at 8441-42	30
§ 4(b), 90 Fed. Reg. at 8442	20

**Other Authority:**

Restatement (Second) of Torts (A.L.I. 1977), Westlaw (database updated Oct. 2024):	
§ 652B	4, 5, 7, 9
cmt. a	5

## INTRODUCTION

As explained in the government’s opening brief, the district court’s conclusion that plaintiffs here are likely to succeed on the merits of their claims suffers from numerous, independently fatal errors. The district court based standing on a theory of injury that materially differs from that accepted in any other case from this Court or any other. It identified final agency action notwithstanding the fact that the action at issue—internal agency decisions to hire employees, onboard them, and give them access to agency data systems—is nothing like the agency action at issue in any other case plaintiffs or the district court ever identified. And in concluding plaintiffs were likely to succeed on their Privacy Act claim, the district court relied on a novel reading of the statute that no court has ever accepted. In every respect, the district court’s preliminary injunction is unsupported by law or precedent.

That conclusion is confirmed by the Supreme Court’s grant of the government’s application to stay the district court’s preliminary injunction. *See Social Sec. Admin. v. American Fed’n of State, Cnty., & Mun. Emps.*, 145 S. Ct. 1626 (2025). That decision necessarily means

that a majority of the Justices concluded that each of the stay factors articulated in *Nken v. Holder*, 556 U.S. 418, 434 (2009)—including that *the government* had established a substantial likelihood of success on the merits—was satisfied. Plaintiffs cannot square the Supreme Court’s stay decision with their insistence that the district court was nevertheless correct to hold that plaintiffs are substantially likely to succeed on the merits. The preliminary injunction should be vacated.

### ARGUMENT

As explained in the government’s opening brief, plaintiffs’ claims face numerous independent barriers, any one of which is fatal to plaintiffs’ likelihood of success on the merits. Because plaintiffs cannot establish that they are likely to prevail on any of the threshold and merits issues presented—let alone all of them—they necessarily cannot make a “clear showing” that they are likely to succeed on the merits. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008). The preliminary injunction should be vacated.

## **I. Plaintiffs Have No Likelihood of Success on the Merits**

### **A. Plaintiffs fail to establish a cognizable Article III injury**

1. Plaintiffs fail to establish standing because they have not identified a cognizable injury under the standards set out in *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). There, the Supreme Court explained that an intangible harm may be cognizable for standing purposes only when it “has a ‘close relationship’ to a harm traditionally recognized as providing a basis for a lawsuit in American courts.” *Id.* at 417 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). Plaintiffs agree that *TransUnion*’s framework applies, Resp. Br. 19 (Resp.), that the only “traditional[]” analogue the district court accepted is the tort of intrusion upon seclusion, Resp. 20, and that the appropriate starting point for analyzing that tort is the Restatement (Second) of Torts § 652B, *see* Resp. 21. As we explained in our opening brief, Br. 27-34, an agency affording its own employees access to (lawfully obtained) information contained in data systems the agency (lawfully) operates and maintains is in no way analogous to a “highly offensive” “intentional[] intru[sion], physical[] or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.” *See*



Restatement (Second) of Torts § 652B (A.L.I. 1977), Westlaw (database updated Oct. 2024) (Restatement). In fact, plaintiffs do not allege that they would even know if a record containing their personal information was accessed, barring some step taken by the agency to alert plaintiffs of the fact.

2. Plaintiffs barely explain why they think intra-agency access to agency files is a “highly offensive” intrusion. Instead, they devote a great deal of their response to propositions no one contests. The government has never argued that intangible harms can never form the basis of standing, Resp. 19-20, that this Court should deviate from the formulation of the tort given in the Restatement (Second) of Torts, Resp. 20-21, that intrusion upon seclusion must be physical in nature, Resp. 22-23, or that the intrusion must be into the plaintiff’s home, Resp. 26-28. None of those points is contested in this case.

Nor do plaintiffs respond to numerous arguments that *do* appear in our opening brief. Plaintiffs offer no response to our observation (Br. 31-32) that the notes to the Restatement explicitly provide that “[l]ocating and supplying information for one’s own files” is not an actionable intrusion, Restatement § 652B Reporter’s Note, or to the

cases cited by both our brief and the Restatement rejecting liability where the intrusion complained of is an internal review of an entity's own files and where there is no suggestion that the information contained in those files was unlawfully obtained or retained, *see Tureen v. Equifax, Inc.*, 571 F.2d 411, 416 (8th Cir. 1978). Plaintiffs effectively concede that, if they prevail, this would be the first case to hold that an individual is injured by allowing an employee to access internal, lawfully obtained records.

3. Plaintiffs' theory of injury also diverges from the common law tort because plaintiffs do not allege that DOGE team members have targeted their members' information or will ever even look at *their* information. Opening Br. 33. That is difficult to square with the Restatement's description of an "intentional[] intrusion" into an individual's "solitude or seclusion." Restatement § 652B & cmt. a (referring in the singular to "the person" and "his" privacy interest). Plaintiffs' observation (Resp. 23) that this Court has never found "individual 'targeting'" to be necessary under the common law is accurate but misleading: Plaintiffs identify no prior case where that kind of targeting was lacking, so this Court never had to confront the

question. Thus, plaintiffs' observation only underscores the novelty of their theory of injury.

Plaintiffs fare no better in suggesting in passing that they could demonstrate that kind of targeting if it were required. Resp. 24. It is plaintiffs' burden to demonstrate standing, and the mere fact that the record shows that DOGE team members have reviewed *some* individual records falls far short of demonstrating that the team has in any way targeted, reviewed, or even accessed the records of any of plaintiffs' members, as Article III demands. *Powers v. Ohio*, 499 U.S. 400, 410-11 (1991) (noting plaintiffs' general inability to sue to vindicate third-party rights).

4. Plaintiffs' attempt to reconcile their position with this Court's precedent is equally unavailing. As we explained, the kind of intrusion this Court deemed sufficient to establish standing in *Krakauer v. Dish Network, LLC*, 925 F.3d 643 (4th Cir. 2019), and *Garey v. James S. Farrin, P.C.*, 35 F.4th 917 (4th Cir. 2022), is nothing like the kind of intrusion alleged here. Br. 34-40. Plaintiffs respond that those cases do not require a physical invasion into a plaintiff's space. Resp. 26-28. That is true but unresponsive. The problem is not

that plaintiffs fail to allege a physical invasion. As explained, *supra* pp. 3-5, it is that the action they challenge (internal review of data legally contained in agency systems housed and maintained by the agency) does not involve any “intentional[]” “invasion” into plaintiffs’ “solitude or seclusion,” let alone in a manner that would be “highly offensive.” Restatement § 652B.

Plaintiffs and the district court wrongly read *Krakauer* and *Garey* to suggest that the presence of private information alone makes plaintiffs’ theory sufficiently analogous to intrusion upon seclusion. Resp. 28. In both cases, the defendants intentionally obtained the plaintiffs’ information in a manner that the plaintiffs objected to, then used that information in a manner that concretely intruded into the plaintiffs’ private space. *See Krakauer*, 925 F.3d at 653 (“Cognizable intrusions include intrusions made via phone calls.”); *Garey*, 35 F.4th at 921 (describing standing question as “nearly identical” to that raised in *Krakauer*). That is a world away from agency employees merely being given access to internal data systems subject to the normal legal and ethical obligations to maintain the confidentiality of those records. *See* 5 U.S.C. § 552a(i)(1) (Privacy Act section imposing criminal penalties

for knowingly and willfully disclosing personally identifiable information (PII) in violation of the statute). And as noted above, *supra* pp. 4-5, other courts and the Restatement have recognized that mere access to private information lawfully contained in the defendant's own files is not a tort. *See Tureen*, 571 F.2d at 416.

Plaintiffs' reliance on *Garey* is particularly inapposite given that the Court there held that the plaintiffs did not have standing to seek injunctive relief—the only form of relief at issue in this appeal. Just as in *Garey*, plaintiffs' "theory of the case, the obtaining of their personal information[,] is a *fait accompli*." 35 F.4th at 923. Plaintiffs acknowledge that the decision to allow DOGE team members to access these systems was made six months ago and that team members had access to those systems before any injunction ever issued in this case. *Garey* concluded that kind of already-accomplished access to private information "does not establish an ongoing or imminent injury" sufficient to "support injunctive relief." *Id.*

Similarly, plaintiffs are wrong to suggest that their case is distinguishable from cases where this Court held there was no standing because the information at issue here is more private than the

information at issue in those cases. Nothing in the Restatement or this Court's precedent suggests that the common law tort of intrusion upon seclusion turns on how private the information at issue is. To the contrary, the Restatement refers generally to "invasion" into an individual's "private affairs or concerns" with no suggestion that the kind of "invasion" required changes based on the kind of information at issue. Restatement § 652B. This Court's precedent is in accord. In *O'Leary v. Trusted ID, Inc.*, 60 F.4th 240 (4th Cir. 2023), this Court did not question the sensitivity and confidential nature of the information at issue—most of the plaintiff's social security number—in rejecting the proffered common-law analogue. Instead, it focused on the defendant's alleged conduct and concluded that the plaintiff had not "alleged an injury with a close relationship to 'intrusion upon seclusion'" because the kind of intrusion alleged was not sufficiently similar to that recognized at common law. *Id.* at 245-46.

That plaintiffs have claimed that they feel "unease" also does not establish injury or distinguish their suit from *AFT v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025). *Contra* Resp. 25 (quoting *Bessent*, 2025 WL 1023638, at \*4 (Richardson, J., concurring)).

Plaintiffs in *Bessent* alleged exactly the same kind of unease. *See, e.g.*, Joint Appendix at JA37, *AFT v. Bessent*, No. 25-1282 (4th Cir. Apr. 14, 2025) (amended complaint alleging plaintiff experienced “distress[]” and “worr[y]”); *id.* at JA60 (alleging “major distress and anxiety”). Asking whether an injury has a historical analogue, as *TransUnion* demands, means asking what type of conduct led to the injury complained of. As in *Bessent*, the subjective unease the plaintiffs experienced does not stem from conduct that historically would have given rise to tort liability. Indeed, that is exactly the holding of *TransUnion*: Subjective discomfort is not enough to establish Article III standing.

Plaintiffs say that the information about them in the agency’s possession is not “voluntarily” shared with the agency because they must share information in exchange for critical benefits. Resp. 33. But that only underscores the government’s point. Plaintiffs do not contest that the agency can lawfully acquire and maintain their information, as they acknowledge the agency *must* do so to provide them with benefits. That already distinguishes this from every invasion-of-privacy case plaintiffs cite, where there was some objection to either the manner or

the fact of the defendant's acquisition of the plaintiff's personal information.

5. Finally, plaintiffs' argument (Resp. 30-32) that Congress's enactment of the Privacy Act can salvage their standing theory runs headlong into the Supreme Court's holding in *TransUnion*. Congress can create "a statutory prohibition or obligation and a cause of action" but may not override Article III's injury requirement. *TransUnion*, 594 U.S. at 426. Whatever Congress might have intended is irrelevant to the question whether plaintiffs have established constitutional standing. As discussed, *supra* pp. 4-5, both the Restatement and case law demonstrate that the common law has never recognized a privacy injury in cases where the allegations are only that a defendant reviewed records and information lawfully obtained and maintained in its own systems. Congress's decision to impose additional statutory requirements on agency decisions to share private information internally cannot create a cognizable injury.



**B. Plaintiffs do not challenge any final agency action reviewable under the Administrative Procedure Act**

To qualify as “agency action,” the action must be an “agency rule, order, license, sanction, relief, or the equivalent.” 5 U.S.C. § 551(13). While that definition is construed expansively, courts have long recognized that this definition of agency action “is not so all-encompassing as to authorize us to exercise ‘judicial review [over] everything done by an administrative agency.’” *Independent Equip. Dealers Ass’n v. EPA*, 372 F.3d 420, 427 (D.C. Cir. 2004) (alteration in original) (quoting *Hearst Radio, Inc. v. FCC*, 167 F.2d 225, 227 (D.C. Cir. 1948)). Agency decisions to grant employees access to internal agency systems are not a “rule, order, license, sanction, ... or the equivalent.” 5 U.S.C. § 551(13). And plaintiffs identify no case where a court has concluded that anything remotely like the agency action at issue here is reviewable. Finding no support in the text of the Administrative Procedure Act (APA) or case law, plaintiffs’ arguments should be rejected. At the very least, this Court should hold that the district court erred in concluding that plaintiffs are likely to succeed on

their novel theory of agency action for the purpose of obtaining a preliminary injunction.

1. As we explained, plaintiffs' complaint seeks review of exactly the kind of day-to-day management of agency operations that has long been held to be outside the scope of the APA. Br. 41-42. The supposed "agency action" plaintiffs identify is a loosely defined series of personnel decisions related to granting individual employees access to agency systems. This Court has held that courts "are woefully ill-suited ... to adjudicate" "attack[s]" "asking [the judiciary] to improve an agency's performance or operations." *City of New York v. U.S. Dep't of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) (quotation omitted). In that kind of case, "courts would be forced either to enter a disfavored 'obey the law' injunction or to engage in day-to-day oversight of the executive's administrative practices. Both alternatives are foreclosed by the APA, and rightly so." *Id.* (citation omitted).

Plaintiffs, like the district court, principally respond by asserting that what they have challenged is a policy, and that policies necessarily can be challenged under the APA. Resp. 34-35. For starters, an *ipse dixit* assertion that a series of individual HR decisions amounts to a

new “policy” does not control whether an action is reviewable under the APA. Whatever label plaintiffs put on it, they acknowledge in their response that what they challenge concerns internal agency hiring and human resources decisions related to the “employment agreements, ... training, ... background investigations,” and systems access decisions for a set of employees hired to do work that plaintiffs evidently disagree with. Resp. 35. As explained in the government’s opening brief, Br. 42, neither the district court nor plaintiffs have ever identified any case allowing an APA challenge to proceed against anything like what plaintiffs challenge here, outside parallel challenges to DOGE data access. Plaintiffs have essentially no response to the novelty of their theory of the scope of APA review.

These features make this case materially unlike *Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925 (D.C. Cir. 2008), an out-of-circuit decision on which both plaintiffs and the district court relied. Resp. 36-37. As noted in the government’s opening brief, Br. 44-45, *Venetian* involved a defined, if unwritten, agency policy of disclosing information submitted by third parties without notification to those individuals. *Venetian*, 530 F.3d at 927. In other words, the policy at issue was a

functional “rule,” *see* 5 U.S.C. § 551(13), in that it was a procedure followed by agency staff with respect to a particular class of data. Here, in contrast, plaintiffs have not identified a defined policy that operates in a specified manner—they instead seek to subject multifarious agency practices to judicial review under the label “policy.”

Plaintiffs do not meaningfully respond to our argument that the district court’s expansive understanding of agency action would subject virtually every aspect of agencies’ day-to-day management of internal operations to APA review. *See* Opening Br. 42. Plaintiffs assert that changes to agency policies differ from the many ways agencies “follow” their policies in the course of their day-to-day operations. Resp. 35 (emphasis omitted). But plaintiffs do not explain why that theoretical distinction matters and cite no support for it. *Id.* In fact, as reflected in plaintiffs’ brief, the limitation plaintiffs propose on their theory is no limit at all. If plaintiffs retain their preliminary injunction without having cited any record evidence that an agency has in fact made a “decision” to change policy, Resp. 36—as opposed to evidence that an agency has merely continued to operate day to day—future plaintiffs will be able to challenge internal agency workings under the APA

simply by asserting that the day-to-day operations they object to are part of a policy.

2. Even if the plaintiffs challenge “agency action,” the action they challenge is not “final” for APA purposes. As we explained, internal data access decisions do not impose obligations, regulate plaintiffs conduct, or otherwise impose any direct legal consequences for plaintiffs or anyone else. Br. 43-45. Here, too, plaintiffs continue to rely on the D.C. Circuit’s decision in *Venetian*, 530 F.3d 925, for the proposition that “polic[ies]” involving data access decisions are necessarily final and reviewable under the APA. Resp. 36-37. But as we explained, Br. 44-45, that case involved an agency’s “disclosure policy” that authorized employees to disclose confidential information held by the agency to third parties outside the government in certain circumstances. *Venetian*, 530 F.3d at 927. Those disclosures to third parties, once accomplished, had immediate material consequences for the plaintiff. *Id.* Those immediate and obvious “legal consequences,” *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997) (quotation omitted), demonstrated the existence of final agency action. *Venetian* thus says nothing about a case, like this one, that involves only an agency’s

entirely internal actions in allocating access to agency information among employees.

\* \* \*

A final note about the threshold problems with plaintiffs' claims: Contrary to plaintiffs' suggestion (Resp. 30-32, 35), rejecting these claims does not mean that the Privacy Act's protections are toothless or that plaintiffs are without recourse to protect their private information. To the contrary, the Privacy Act provides for a comprehensive remedial scheme that expressly gives plaintiffs—or anyone else—the right to seek damages for a “fail[ure] to comply” with “any ... provision” of the Act if that failure damages an individual. 5 U.S.C. § 552a(g)(1)(D), (4). The statute further provides for additional damages if the violation was “intentional or willful.” *Id.* § 552a(g)(4). And any employee who knowingly and willfully discloses PII in violation of the statute can be subject to criminal penalties under the Act. *Id.* § 552a(i)(1).

Thus, rejecting plaintiffs' claims at the threshold does not undermine the purposes of the Privacy Act. Consistent with the demands of Article III, Congress has concluded that the Privacy Act's requirements are not to be enforced by roving injunctions controlling

internal agency practices, but instead by the threat of damages suits that hold the government accountable for any harm those practices might cause.

**C. Plaintiffs’ Privacy Act and APA claims fail on the merits**

Even if plaintiffs’ claims were justiciable, they would fail on the merits. The district court addressed only two of those claims: (1) that “[the Social Security Administration’s (SSA)] provision to the DOGE Team of access to SSA systems is ‘not in accordance with’” law—*i.e.*, the Privacy Act—because defendants had failed to establish the employees’ need to access the relevant databases and (2) that defendants’ failure to establish the DOGE employees’ need rendered the decision to grant them access unreasonable, in violation of the APA. JA1435-1436. Those related holdings are both erroneous.

**1. Privacy Act claim**

a. As plaintiffs note, the Privacy Act was enacted to control the “collection, maintenance, use, and dissemination” of private information by federal agencies. Resp. 38 (quotation omitted). Plaintiffs, however, have no objection to the collection of their information by SSA, nor to SSA’s maintenance of that information in their systems. Nor do they

dispute that the Privacy Act authorizes SSA's employees to use that information when the agency concludes the employees need access to accomplish their work. And plaintiffs accept that—for as long as these systems have existed—numerous SSA employees have had access to the private information contained in them pursuant to that exception. Instead, plaintiffs object only to their information being used by the agency for a specific purpose that they evidently disagree with—the modernization of agency systems mandated by the President's Executive Order—by a particular set of employees hired to carry out that work. Plaintiffs cite no Privacy Act case raising anything like that kind of second-guessing of agency decision-making about what is necessary to achieve its mission. And it is far afield from anything Congress had in mind when it enacted the Privacy Act.

b. Plaintiffs, like the district court, rely heavily on a repeated assertion that SSA did not explain why DOGE team members needed to be given system access to accomplish their mission. Resp. 43-48. As we explained, that argument is entirely refuted by the very presidential directive that created the DOGE team. Br. 48-53. That Executive Order directed DOGE teams to undertake an ambitious operation “to



improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems.” Exec. Order No. 14,158, § 4(a), 90 Fed. Reg. 8441, 8441 (Jan. 29, 2025). That work would include, “[a]mong other things,” “promot[ing] interoperability between agency networks and systems, ensur[ing] data integrity, and facilitat[ing] responsible data collection and synchronization.” *Id.* In order to improve government systems, the executive order unsurprisingly directed agencies to give DOGE team members “full and prompt access” to the systems they were directed to improve, subject at all times to “rigorous data protection standards.” *Id.* § 4(b), 90 Fed. Reg. at 8442.

Plaintiffs respond that Executive Orders cannot by themselves license a violation of the law. Resp. 44. But that entirely misses the point of the government’s argument. The Privacy Act indisputably allows agency employees to access information in agency systems when they have a need to do so, and DOGE team members needed access to SSA systems because the President had directed them to review and improve those systems. Plaintiffs have never contested that directive is a legitimate one, or that improving the efficiency of data systems is a

valid objective for purposes of demonstrating a need-to-know under the Privacy Act. *See* Opening Br. 6 (discussing Government Accountability Office reports about waste). That distinguishes this case from *Parks v. U.S. IRS*, 618 F.2d 677 (10th Cir. 1980), where the directive at issue (blacklisting and pressuring federal employees to buy bonds) was “expressly held out” by Congress as an illegitimate purpose not considered to be part of “federal employees’ regular duties.” *Id.* at 681 & n.1.

Plaintiffs alternatively assert that a “generalized directi[ve] to the whole of government is not sufficient to meet the Privacy Act’s standard that individual agencies determine the need” that would justify records access. Resp. 44. Plaintiffs misconstrue the statute. The Privacy Act does not require each agency to make its own independent need determination when need is expressly directed by Executive Order; it merely says that each employee must “have a need ... in the performance of [his] duties.” 5 U.S.C. § 552a(b)(1). Plaintiffs give no reason why the President, as head of the Executive Branch, cannot simultaneously establish the “need” required by the Privacy Act for a group of employees engaged in an important project across numerous

agencies. *See Seila Law LLC v. CFPB*, 591 U.S. 197, 203 (2020)

(“Under our Constitution, the ‘executive Power’—all of it—is ‘vested in a President,’ who must ‘take Care that the Laws be faithfully executed.’” (quoting U.S. Const. art. II, § 1, cl. 1; *id.* § 3)).

Finally, plaintiffs suggest that there is some inconsistency between the government’s reliance on the Executive Order and evidence submitted below. *See* Resp. 47-48. Not so. The individual projects identified in declarations below, like detecting fraud in government payment systems, fall comfortably within the Executive Order’s directive “to improve the quality and efficiency” of government systems and “ensure data integrity” in those systems. Exec. Order No. 14,158, § 4(a), 90 Fed. Reg. at 8441. That the DOGE team’s broad review of agency data systems matured into more targeted projects over time as the team identified particular areas of inefficiency is consistent with the discussion above, *supra* pp. 19-20, about the nature of the team’s need.

c. Pivoting from their attack on the relevance of the Executive Order, plaintiffs critique the level of access provided to the DOGE team, asserting that it is disproportionate to any need that might exist. As we explained, though, it is not difficult to understand why the DOGE team

needed full access to the systems they were tasked with improving in order to improve them. Opening Br. 49. That the reason is easy to explain and understand does not mean, as plaintiffs assert, that “the government makes no effort to explain why access” to the data is needed. Resp. 43.

A hypothetical helps demonstrate the commonsense proposition. Imagine a new employee is hired by a company to figure out how to improve the company’s billing system. The new employee is not familiar with that system or the company’s existing practices, and that’s the whole point. The company’s leadership and existing employees have been unable to improve the efficiency of the system themselves and have decided to hire a fresh set of eyes—perhaps with some special expertise or skill set—to come in, take a top-to-bottom look at the system, identify potential inefficiencies or problems, and then try to fix them. The new hire will plainly “need” full access to every aspect of the system to perform that review. Requiring the employee to first articulate a concrete reason why they need access to particular data within the system would defeat the entire point of the endeavor. The

new employee will not know where the problems or inefficiencies are until he identifies them.

That kind of broad, holistic review of government systems is exactly what is mandated by the Executive Order, and that is sufficient to demonstrate that DOGE team members needed full access to SSA systems in order to do their job. In fact, elsewhere in their brief, plaintiffs tacitly acknowledge that “unfettered” or “sweeping” access, Resp. 44, 45, can be justified under the Privacy Act, noting that the kind of access granted to the DOGE team members has long been granted to “30 to 40” other employees of the agency, Resp. 45; *see also* Resp. 48 (expressing the view that the Privacy Act permits “non-DOGE Team SSA employees[]” to access large swaths of SSA information that contains PII). But for reasons plaintiffs never explain, they insist that *DOGE team* employees cannot possibly justify the same access.

d. Plaintiffs’ contrary position, like the district court’s, rests in significant part on a reading of “need” to mean not just “need-to-know” but “need with no available alternative.” Plaintiffs refer, for example, to evidence suggesting that the agency might have complied with the Executive Order in a more restrictive manner, whether by anonymizing

data to the maximum extent possible or by limiting initial grants of access to data and subsequently expanding the scope of access. Resp. 42-44. But the Privacy Act asks only whether the employees in question had a “need” for the access given in order to do their jobs. To read “need” as plaintiffs do contorts the normal usage of the word. When someone says “I need to go to the grocery store,” everyone understands that means the person has a concrete reason for doing so. No one would object that the person doesn’t “need” to go to the store because they could use whatever groceries are already on hand or have their groceries delivered instead.

Unsurprisingly, plaintiffs are able to identify no decision outside the context of this and related litigation in which a court has read “need” so narrowly. Plaintiffs incorrectly assert that *Bigelow v. Department of Def.*, 217 F.3d 875 (D.C. Cir. 2000), *cert. denied*, 532 U.S. 971 (2001), supports their reading. Resp. 46. To the contrary, *Bigelow* would have come out the other way under plaintiffs’ understanding of the statute. There, a supervisor accessed his subordinate’s personnel security clearance file to assuage “doubts” the supervisor had about his subordinate’s trustworthiness. *Bigelow*, 217 F.3d at 877. The D.C.

Circuit concluded that was enough to demonstrate a “need” notwithstanding that the supervisor would not ordinarily have access to those files, he did not have any authority to review or modify the subordinate’s security clearance, and that there were “various [other] ways of fulfilling the supervisor’s duty” to “assur[e] the trustworthiness” of a subordinate provided for by regulation. *Id.* Under the district court’s understanding of the statute, the *Bigelow* court could not have found a “need” under those facts because the supervisor’s decision to look at his subordinate’s security file was not strictly necessary—the supervisor could have instead addressed his concerns by, for example, “forward[ing]” them to a separate office that was “responsible for reviewing” security concerns “and determining whether” further action was warranted. *Id.* at 879 (Tatel, J. dissenting).

Plaintiffs’ novel understanding of the Privacy Act runs counter to that most natural understanding of “need” and should be rejected. But plaintiffs go even further and assert that, when assessing need, courts can disregard whether the access the agency granted was necessary to do its work in an expeditious and efficient manner. Plaintiffs dismiss out of hand evidence showing that the agency’s work would have taken

longer if it had cabined or anonymized employees' data access and question why an agency should be permitted to "determin[e] ... the speed at which it wishes to do its work." Resp. 46. The answer should be obvious—because it is the Executive Branch, not private litigants, that executes federal law.

e. In addition to reading "need" too narrowly, plaintiffs assert that the Privacy Act requires an agency to show a separate need for disclosure of each item of PII within a record. Resp. 41. Once again, plaintiffs identify no case in the more than 50 years the Privacy Act has been in effect applying anything like that standard. And again, plaintiffs' reading is belied by the plain text of the statute, which permits disclosure to "employees of the agency which maintains the record who have a need for the *record*[" 5 U.S.C. § 552a(b)(1) (emphasis added). As explained, *supra* pp. 22-24, the employees at issue here needed broad access to the records contained in the agency's records systems in order to review and modernize those systems.

In addition to being unsupported by precedent or case law, it is difficult to imagine how an employee would ever be authorized to look at an agency record that contains PII under plaintiffs' reading. Suppose



a form lists a person's name, age, height, and weight, in addition to other information. Under plaintiffs' approach, unless an employee can demonstrate a particularized "need" to know the person's height and weight—"item[s] of information about an individual" that, per plaintiffs reading, Resp. 41 (quotation omitted), would be separate "records"—they would be prohibited from looking at the form without first undergoing burdensome redaction. That kind of supervision of internal agency redaction and anonymization processes has no basis in the text of the statute and would result in an unworkable system under which employees performing all kinds of basic tasks would be prohibited from doing so, or only authorized to do so after engaging in a protracted process to determine which fields within a record are not strictly necessary for their work.

All told, plaintiffs' novel reading of the Privacy Act creates onerous requirements that appear nowhere in its text or in case law interpreting it. No court has ever interpreted the Privacy Act to require anything like what plaintiffs propose. And that is not surprising, as the standard plaintiffs propose would authorize a shocking and unworkable intrusion into the inner workings of federal agencies. To permit that

intrusion here would lead to disruptive and absurd results, transforming the Privacy Act into a *de facto* private-party veto over any decision by an agency to allow its employees to access information in order to do their jobs.

f. Finally, plaintiffs' argument that they are likely to show DOGE team members are not employees of SSA for Privacy Act purposes is incorrect. Resp. 48-50. "For the purpose of" Title 5 of the U.S. Code—which includes the Privacy Act—"employee" means "an officer and an individual who is" first "appointed in the civil service by," *inter alia*, "the President" or "an individual who is an employee under this section." 5 U.S.C. § 2105(a)(1)(A), (D). An employee must also be "engaged in the performance of a Federal function under authority of law or an Executive act" and "subject to the supervision of an individual named by paragraph (1) of this subsection while engaged in the performance of the duties of his position." *Id.* § 2105(a)(2), (3). The SSA DOGE team members satisfy that definition, and the district court did not hold otherwise. *See* JA1416 (assuming that the relevant team members "have 'intra agency' status at SSA"); *see also* Exec. Order No. 14,158, § 3(c), 90 Fed. Reg. at 8441 (directing agency heads to "establish

within their respective Agencies a DOGE Team of at least four employees”).

Plaintiffs’ speculation that someone other than SSA leadership “must be” directing (and therefore, presumably, employing) the SSA DOGE team is meritless. An isolated statement (Resp. 49) from the SSA Commissioner that USDS itself has some authority to provide direction for the modernization project it is charged with overseeing, Exec. Order No. 14,158, §§ 3(b), 4(a)-(b), 90 Fed. Reg. at 8441-42, is not novel or troublesome—it is precisely how the President intended the project to operate. And it does not make the DOGE team at SSA any less employed by the agency because they “coordinate” with USDS. Resp. 50.

## **2. Arbitrary and capricious claim**

As plaintiffs acknowledge, review under the APA is “highly deferential, with a presumption in favor of finding the agency action valid.” *Ohio Valley Env’t Coal v. Aracoma Coal Co.*, 556 F.3d 177, 192 (4th Cir. 2009). Moreover, “the ultimate standard of review is a narrow one,” as “[t]he court is not empowered to substitute its judgment for that of the agency.” *Id.* (quotation omitted). Even assuming the hiring

and data access systems that plaintiffs identify are properly subject to that kind of review at all, *but see supra* Part I.B, the agency actions here easily satisfy that standard.

Many of plaintiffs' arguments about their arbitrary and capricious claim overlap with arguments already addressed. Plaintiffs complain that the administrative record here does not reflect that the agency made a considered decision to change its policies for the hiring, onboarding, training, and access protocols for the DOGE team. But as explained above, there is no evidence of such a change in policy because no such policy change was made. *See supra* pp. 12-15. Indeed, plaintiffs acknowledge that what the administrative record *does* show only supports that conclusion. *See Resp.* 52-55. The record shows that the data-access decisions that plaintiffs challenge were not the result of some broad policy but instead the result of individual email conversations reviewing and processing DOGE team members' requests for data access. *See Resp.* 57-61.

To the extent plaintiffs' argument boils down to an assertion that the mere fact that access was *granted* to DOGE team members demonstrates that the agency must have departed from normal

practice, that argument is meritless. Plaintiffs concede that “30-40” other employees “have access akin to what the DOGE Team requested and obtained,” Resp. 60, demonstrating that the level of access plaintiffs complain of is available under the agency’s normal procedures. To the extent the degree of access granted is unusual, as explained at length above, *supra* pp. 18-24, that only reflects the unusually broad mission the DOGE team was tasked with and does not provide a basis to declare the agency’s decisions arbitrary and capricious.

Plaintiffs alternatively argue that the administrative record fails to show that individual employees considered “reliance interests” (Resp. 56) or “policy alternatives” (Resp. 57-59) when they were asked to make run-of-the-mill decisions about onboarding new employees and processing requests for access to data systems. But again, that only reflects that the “agency actions” at issue here are routine, internal personnel decisions. For the reasons already given, *supra* Part I.B, those internal agency human resources and staffing decisions are not subject to APA review, and indeed it would be shocking if that kind of day-to-day operational decision making by individual human resources

personnel could be successfully challenged in court for failure to consider reliance interests and policy considerations.

## **II. Plaintiffs Also Fail to Establish the Remaining Preliminary Injunction Factors**

The remaining factors—irreparable harm, the balance of harms, and the public interest—likewise favor the government and fail to support the district court’s injunction. Unsurprisingly, plaintiffs’ arguments on each of those factors merely restate their arguments on the merits. *See* Resp. 50-56. And plaintiffs do not seriously contest that, if they are not likely to succeed on the merits of their claims for any reason, they also cannot satisfy the remaining requirements for an injunction.

Even if plaintiffs were likely to prevail on the merits, the remaining factors would not support a preliminary injunction. The district court’s injunction thwarts the government’s implementation of a vital presidential initiative. And reinstating the injunction, after the DOGE team has already conducted its work for nearly two months under the Supreme Court’s stay order, would derail that effort midstream. Conversely, plaintiffs experience no harm, let alone irreparable harm, from the mere fact that DOGE team members, like

other agency employees, can access databases containing plaintiffs' personal information subject to the normal legal and ethical obligations that attend that kind of access. The balance of the equities and the public interest thus strongly favor allowing the important work of the DOGE team employees to proceed.

## CONCLUSION

For the foregoing reasons, this Court should vacate the preliminary injunction.

Respectfully submitted,

BRETT A. SHUMATE,  
*Assistant Attorney General*  
YAAKOV M. ROTH  
*Principal Deputy Assistant  
Attorney General*

ERIC D. McARTHUR  
*Deputy Assistant Attorney  
General*

BRAD HINSHELWOOD

/s/ Jack Starcher  
JACK STARCHER  
SIMON JEROME  
JACOB CHRISTENSEN  
*Attorneys, Appellate Staff  
Civil Division, Room 7515  
U.S. Department of Justice  
950 Pennsylvania Avenue NW  
Washington, DC 20530  
(202) 514-8877*

July 2025



## CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 6,464 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Word for Microsoft 365 in Century Schoolbook 14-point font, a proportionally spaced typeface.

s/ Jack Starcher  
Jack Starcher

**CERTIFICATE OF SERVICE**

I certify that on July 30, 2025, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Service will be accomplished by the appellate CM/ECF system.

*s/ Jack Starcher*  
\_\_\_\_\_  
Jack Starcher